International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 4, May-June 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Crime and Challenges Ahead

Dr. S. Krishnan[1], Ms Rakshita Chaturvedi[2]

[1]Associate Professor, [2]Student,
[1,2]Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

How to cite this paper: Dr. S. Krishnan | Ms Rakshita Chaturvedi "Cyber Crime and Challenges Ahead" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-4, June 2021, pp.347-357, URL: www.ijtsrd.com/papers/ijtsrd41279.pdf

IJTSRD41279

INTRODUCTION:

The World War I saw gas war as a new weapon. This was banned under the Geneva Convention. The World War II saw nuclear or the atomic bomb as the weapon of war. A single bomb could devastate the whole city. Now, we can expect the next war to be the e-war (ie. cyber war). In this type of war there is less physical risk of men to deploy weapons of destruction. A person sitting in any safe corner of the world in his own country can paralyze or destroy the infrastructure of the enemy country by hacking its network system and by infecting it with deadly virus without formally declaring any war.

With the advent of the new technologies and the advancement in the mode of communications, the Internet has become a new form of life. It is one of the fastest modes of communication and has spread its tentacles, covering all possible shades of mankind. But as the saying goes, "every good side has a bad side too". The same is true with computers, the Internet technology. The advent of the computer has been a boon to students, lawyers, businessmen, teachers, doctors, researchers and also not to forget the criminals. Today we venture into the virtual world of cyber-space where our privacy does not exist at all. What you share, in good faith, can be exploited against you. Crimes are no more confined to the physical space alone but have entered into the virtual cyberspace too. The weapons which are used to commit these crimes are highly sophisticated and as the criminals are always one step ahead of the law enforcers as they themselves agree, detecting these criminals and preventing their crimes is one of the greatest challenges before them.

Cybercriminals use the internet and computer technology to hack user's personal computer's, smartphone data, personal details from social media ,business secrets, national secrets etc. Criminals who perform these illegal activities through the internet are called hackers. Though various agencies are trying to tackle this problem, it is growing regularly and many people have become victims of identify theft, hacking and malicious software. One of the best ways to stop these criminals and protect sensitive information is by making use of inscrutable security that uses a unified system of software and hardware to authenticate any information that is accessed over the Internet.

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed. lawfully or otherwise. Internationally, both governmental and non- state actors engage in cybercrimes, including espionage, financial theft, and other cross- border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation –state is sometimes referred to as Cyber warfare.

Cybercrime is a criminal activity in which computers or computer networks are used as a tool, a target or a place of criminal activity and includes everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.

Cyber crime is the most dangerous of all the other types of crimes as it causes a huge amount of the loss which is evident from the number of cases coming before the criminal justice system. At the same time it very easy to commit this crime by maintaining anonymity. It does not recognize any geographical boundaries. This makes the investigation, collection of evidence and prosecution of criminals extremely difficult. If these crimes are not curbed in time it may cause a huge loss to the humanity at large.

Definition of Cyber Crime:

Cyber Crime has not been defined anywhere in the Information Technology Act, 2000. But it can be generally defined as an unlawful act where in the computer is either a tool or a target or both.

United Nations' Definition of Cybercrime: At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus:

A. Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
B. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

These definitions are complicated by the fact that an act may be illegal in one nation but not in another.

Cybercriminals buy and sell malware online while also trading in services that test how robust a virus is, business intelligence dashboards to track malware deployment, and tech support. The professionalization, proliferation of cybercrime adds up to countless costs in damages every year, impacting individuals, businesses, and even governments. Experts estimate that cybercrime damages will reach $6 trillion annually by 2021, making it one of the most lucrative criminal enterprises.

As the Internet of Things(IOT) evolves and smart devices become more popular, cybercriminals benefit from a much broader attack surface – increased opportunities to penetrate security measures, gain unauthorized access, and commit crimes.

As the saying goes, there's more than one way to skin a cat – and there are most certainly a variety of ways to make money as a cybercriminal.

Cybercriminals always opt for an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where a huge amount of money flows daily and hack sensitive information. Catching such criminals is difficult. Hence, that increases the number of cyber-crimes across the globe. Computers are vulnerable, so laws are required to protect and safeguard them against cybercriminals. We could list the following reasons for the vulnerability of computers:

- **Easy to access –** The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of breach due to the complex technology. Hackers can steal access codes, retina images, advanced voice recorders, etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.
- **Capacity to store data in comparatively small space-** The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for the people to steal data from any other storage and use it for their own profit.
- **Complex-** The computers run on operating systems and these operating systems are programmed of million of codes . The human mind is imperfect, so they can do mistakes at any stage. Cybercriminals take advantage of these gaps.
- **Negligence-** Negligence is one of the characteristics of human conduct . So, there may be a possibility that protecting the computer system we may make any negligence which provides cybercriminal access and control over the computer system.
- **Loss of evidence-** The data related to the crime can be easily destroyed. So, loss of evidence has become a very common & obvious problem which paralyses the system behind the investigation of cybercrime.

Why Cyber Crimes are Committed?

The development in science and technology has exposed computers and internet to various kinds of modern crimes. Some of the reasons for the rapid increase of cyber crime are: a) the capacity of computers to store large data in a small space, b) This data can be accessed very easily – this is done by implanting the computer system with logic bombs, c) Negligence by users – while protecting the computer system the user might be negligent, this gives the cyber criminal to grab the opportunity to gain unauthorised access and control over the computer system, and d) Loss of evidence - the data stored on the computers can be easily destroyed becomes a great hindrance to the investigation agency and may cause loss of evidence.

Who are cyber criminals?

The classification of cyber criminals are on the basis of the object that they have in their mind while commting such crimes. Some of the cyber criminals include criminals such as:

A. Children and adolescents between the age group of 6 – 18 years because of their tendency to know and explore the things and sometimes to prove their unique qualities,

B. organised hackers – they have their own targets to achieve,

C. Professional hackers or crackers – they are employed to hack the site of the rivals and get credible, reliable and valuable information,

D. Discontented employees – these people include those who have been either sacked by their employer or are dissatisfied with their employer. Therefore to take a revenge they resort to these kind of criminal activities.

A wide spectrum of delinquencies come under the umbrella term of 'cyber crime'. At an Internet cafe in China. A wide spectrum of delinquencies are covered under the umbrella term of 'cyber crime', and it is possible that the volume and nature of the crimes would demand in course of time a variety of laws to counter them.

Types of Cyber Crimes: Following are the various types of Cyber Crimes that are specifically mentioned by the IT Act, 2000:

1. Tampering with computer source documents:

Process of intentionally, concealment, destruction, alteration any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law. In *Cox* v *Riley(UK)* there was a deliberate eraser by a disgruntled employee of a computer program from a plastic card controlling a computerized saw, so as to render the saw inoperable. Stephen Brown LJ found that the card was indeed damaged and it has been deprived of its usefulness and it would take both time and money to remedy the situation.

2. Hacking with computer system:

In layman's point of view hacking means to beat the security of a system to gain entry into it without authority. It is usually done by stealing or guessing a password or tricking the program which checks for a password with some smart answers. In *Donald Gene Burleson* v. *The State of Texas*, Burleson, a senior programmer / analyst, was terminated from the services from his company USPA. He knew the passwords of USPA's computer operators used to sign on to the system.

He wanted to take revenge and hence created a program which was responsible for the deletion of important records stored on the systems and the shutting down the entire

system for four hours. He was held to be guilty of hacking the company's computer system and for destroying its records.

3. Publishing of information which is obscene in electronic form:

It refers to the publication or transmission in the electronic form any material which is obscene. In a landmark judgment of *United States vs. Thomas* (1996) the defendant ran a website where members could download photographs unto their computer and even order obscene videos which were delivered to their home. He was held responsible to transmission of obscene material in areas where it was prohibited.

4. Protected System:

Any person who secures access or attempts to secure access to a protected system without any authorisation is liable to be punished with imprisonment which may extend to ten year and also with fine. The Government can declare almost all the Certifying Authority sites as protected because all these sites are critical to the nation since they will be drivers of commerce.

5. Breach of confidentiality and privacy:

Any person who, secures access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned or discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable to be punished under the Information Technology Act. In *Mc Gregor* vs. *Procurator Fiscal of Kilmarnock* the neighbour of a police officer was concerned about the man with whom his 18 year old daughter was living and requested the police officer to find out information for him. McGregor was able to obtain the information from both the Police National Computer and Scottish Criminal records computer. But it was found that he has used the information for the purpose other than that for which registration has been made. He was found guilty of committing a breach of confidentiality and privacy.

Cyber crimes other than those mentioned under the IT Act, 2000.

1. Child Pornography: It is one of the gravest offences The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. Internet explosion has made the children a viable victim to the cyber crime. The pedophiles use their false identity to trap children and even contact them in various chat rooms where they befriend them and gain personal information from the innocent preys. These pedophiles drag children to the net for the purpose of sexual assault or so as to use them as a sex object.

2. Email bombing: refers to sending huge large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing the system or a network.

3. Data diddling: involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

4. Salami attacks: it is a financial crime in which the alteration is so small that it would normally go unnoticed. The *Ziegler case* where a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account is the best example of this type of crime.

5. Virus / worms attacks: Virus is a program that attaches itself to a computer or a file and then circulates to other file and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. The best example of this type of attacks is the case of love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. Almost brought development of Internet to a complete halt.

6. Denial of Service attack (DoS): in this the computer of the victim is flooded with more requests than it can handle which causes its system to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. Some of the examples are websites such as the Amazon, Yahoo, etc.

7. Logic bombs: This crime depends upon a happening of a particular conditional event. The best example is the Chernobyl virus case where a particular virus was lying dormant all through the year and become active only on a particular date.

8. Trojan attacks: A Trojan is an unauthorized program which functions from inside by falsely representing to be an authorized program, thereby concealing what it is actually doing.

9. Internet time thefts: This refers to the usage by an unauthorized person of the Internet hours paid for by another person. This kind of cyber crime was unheard until the victim reported it. This offence is usually covered under IPC and the Indian Telegraph Act.

10. Web jacking: This term has been taken from the word hijacking. Once a website is web jacked the owner of the site looses all control over it. The person gaining such kind of an access is called a hacker who may even alter or destroy any information on the site. E.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded as ransom. Thus web jacking is a process whereby control over the site of another is made backed by some consideration for it.

11. Cyber Stalking: Although there is no universally accepted definition of cyber Stalking, it is generally defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using Internet services. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harms to the victim. It all depends on the course of conduct of the stalker.

12. Cyber squatting: Cyber squatting is the obtaining of a domain name in order to seek payment from the owner of

the trademark, (including business name, trade name, or brand name), and may include typo squatting (where one letter is different).

A trademark owner can prevail in a cyber squatting action by showing that the defendant, in bad faith and with intent to profit, registered a domain name consisting of the plaintiff's distinctive trademark. Factors to determine whether bad faith exists are the extent to which the domain name contains the registrant's legal name, prior use of the domain name in connection with the sale of goods and services, intent to divert customers from one site to another and use of false registration information and the registrant's offer to sell the domain name back to the trademark owner for more than out-of -pocket expenses.

13. Cyber Defamation: Any derogatory statement, which is designed to injure a person's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Besides above list some of the other newly developed cyber crimes include bot, botnets, trojans, backdoors, sniffers, SQL injections, buffer overflows etc.

14. Phishing: it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage.

15. Keystroke Logging: It Is capturing and recording the keystrokes of a user. This kind of tool is used to extract passwords and encryption keys and thus override security measures.

16. Data Driven Attack: A form of attack that is encoded in seemingly harmless data that is executed by a user's or other software to mount an attack. In the case of firewalls, a data-driven attack is a concern as it may get through the firewall in data form and launch an attack against a system behind the firewall.

17. DNS Spoofing: A form of spoofing that exploits the Domain Name Service by which networks map textual domain names on to the IP numbers by which they actually route data packets.

18. Dumpster diving: A form of human intelligence (HUMINT) in which cast-off articles and information are scavenged in an attempt to obtain advantageous data.

19. Electromanetic intrusion: The intentional insertion of electromagnetic pulses into transmission paths in any manner with the objective of deceiving operators or of causing confusion.

Jurisdiction and Cyber Crime:

Without proper jurisdiction the decisions of a court is baseless and ineffective. The main problem with the Internet Jurisdiction is the involvement of multiple parties in different corners of the world. Therefore, it is highly difficult to accurately locate and establish a place from where the offender resides or so as to where the cause of action for the offence has occurred.

Thanks to the legislature that our IT Act, 2000 extends to whole of India and also envisages any offence or contravention there under committed outside India by any person. Hence, it provides for an extra-territorial jurisdiction on Indian Courts and empowers them to take cognizance of offences committed even outside India irrespective of the nationality of the culprit. But in case of foreign criminal belonging to foreign nationals, such offence must involve a computer, computer system on computer network which is located in India.

Nature of Cybercrime

A leading cybercrime scholar, Wall offers useful insights on the nature of cybercrime in his classifications of cybercrime. He categorized cybercrime into four. Namely: cyber trespass, cyber deception/theft, cyber pornography and cyber violence. Cyber trespass entails crossing into other people's property online with a view to causing damage. Examples include: hacking, defacement and viruses attack. Cyber deception/theft has to do with stealing money or property online. Examples include: credit card fraud, phishing e-mails or the violation of intellectual property. Cyber pornography has to do with the violation of obscenity and decency laws online. Example: child pornography. Cyber violence refers to the act of causing psychological harm to or instigating physical harm against others online and in so doing violating human rights laws. Examples include: online hate speech, cyber stalking, etc.

Arguably, the nature of cybercrime can be understood within the broader context of the classification of cybercrime provided by Wall, as explained above. Most variants of cybercrime would fall under the broad four categories. However, the 2016 Internet Crime Report compiled by the Federal Bureau of Investigation (FBI) United States Internet Compliant Centre (IC3) indentified the following types of cybercrimes: Non-payment/non-delivery, personal data breach, 419/overpayment, phishing/vishing/smishing/pharming/employment, extortion, identity theft, harassment/threat of violence, credit card fraud, advanced fee, confidence fraud/romance, no lead value, real estate/rental, government impersonation, business email compromise (BEC)/email account compromise (EAC), tech support, misrepresentation, lottery /sweepstakes, corporate date breach, malware/scareware, ransomware, IPR/copyright and counterfeit, investment, virus, crime against children, civil matter, denial of service, re-shipping, charity, health care related, terrorism, gambling, hacktivist and other.

Causes of Cybercrime

It has been argued that most of the variants of cybercrime that are prevalent today are a reflection of crimes that migrated from the physical space to the cyberspace. The foregoing argument therefore raises the question: why would criminals choose to migrate from the physical space to the cyberspace?

Sheer Curiosity

Young people are fascinated by the Internet and associated digital technologies and are increasingly getting access to them. UNICEF estimates reveal that one third of Internet users around the globe are children; the proportion of Internet users is believed to be likely higher in lower income countries where Internet usage is becoming widespread. Young people are curious by nature and always want to experiment. This curious mindset may lead some intelligent

young people with above average Internet skills to inadvertently engage in deviant and criminal behavior online. For example, they may attempt to guess passwords and try to access someone else's account just for the fun of it or in a bid to 'take a flight of fancy'.

Mischievousness

Mischievousness has been identified as one of the root causes information security incidents in organizations. The act of mischief-making is an age-long phenomenon and as such not new. Mischief makers may employ the Internet as a tool to execute their nefarious activities. This is because the Internet can grant them relative anonymity. Mischief makers who could be current or former employees of an organization, political opponents and former friends of the victim may target an organization or an individual for cyber victimization in order to get even for a perceived wrong.

Peer Influence

Young internet users may be influenced by their peers. Hackers are said to often form social communities with online friends and in quest for acceptance/recognition with these individuals may demonstrate their ability to hack accounts. Arguably, adolescents feel at home within their circle of friends. Because theirs is a world of adventures, they often want to take 'a flight of fancy' and their peers provide an enabling environment for this to happen. Thus, some young people may commit cybercrime damning the consequences just to impress their delinquent peers.

Unemployment

It is argued that employment prevents crime for some people under certain conditions and that employment and criminality relate to each in several ways not only at the aggregate level but also at the individual level. India has an unemployment problem. Unemployment rate has been identified as one of the factors responsible for youth involvement in cybercrime. Some unemployed youth in India are said to be involved in online advanced fee fraud (yahoo-yahoo).

Poverty

The poverty and crime nexus has long been argued in criminological discourses. Field (1990) posits that economic conditions exert countervailing effects on criminal motivation and criminal opportunity. Maslow (1945) identifies physiological needs comprising of the need for food, clothing and shelter as the most fundamental needs of humans. Thus, human beings strive to satisfy these needs and when some cannot access the legitimate means for doing so, they may resort to illegitimate means such as cybercrime. Because there are many unemployed youths in India, there are by extension many poor people in India. Some of these poor youth in order to satisfy their physiological needs may find it convenient to engage in cybercrime.

Second Life Opportunity

The anonymity that the Internet gives users allows people to live out their second lives. Presdee (2000) attributed the increasing rate of crime and disorder in modern society to the political inspiration to people to live two lives. The first life is the formal life that is governed by imposed order, while the second life exhibits the real character of a person. The Internet is said to be encouraging people to live a second life. For example, an otherwise respected person in the society may be involved in online child grooming as he/she may feel comfortable doing so, with a pseudo identity.

Pecuniary Motive

It has been argued that most cybercrime operations entail defrauding the victim for profit. Some people engage in criminal activities online for financial gain. For example, online advance fee fraudsters; popularly referred to as "yahoo-yahoo boys" are primarily motivated by the desire to make fast money from their gullible victims and live extravagant lifestyle. It has been argued that it is relatively easier, less risky, cost- effective to steal information than to rob a bank. Thus, criminals are using ransomware (the digital form of blackmail that involves taking a person's computer hostage) in order to extort money from the person. Digital thieves target consumers as digital baits to rip them off from various malware schemes like ransomware and malvertising.

Revenge Mission

Some individuals may use the Internet as a medium to seek revenge. For example a person may use social networking sites to intimidate his or her former partners. Clough (2015) describes the phenomenon of nonconsensual pornography also known as 'revenge porn' in which intimate images that were consensually taken are eventually uploaded to the Internet or disseminated through social networking sites or website created for such materials to cause a former partner emotional distress. Similarly, cyber attack may be motivated by a quest for revenge for wrong done or perceived to be done to the attacker. The attacker in this instance may be a disgruntled employee, an aggrieved or ex-employee, an ex-partner, a political opponent or a competitor in business. The cyber attack, though extra-judicial may just be their way of getting even with the victim.

Organized Criminal Interest

It is noted that organized crime groups (OCGs) that carried out traditional activities are now utilizing the new criminal opportunities that the internet creates for criminal ends. The internet offers an opportunity structure for decentralized, flexible networks of loosely organized criminal's partner in the distribution of work based on knowledge and skills.There are enough motivations for organized criminal groups to employ the internet architecture for criminal gains. One of such reasons is that the Internet guarantees them anonymity and drastically reduces their risk of doing "business" as their chances of apprehension are relatively low.

Political Interest

Cyber attacks may be politically motivated. They can be sponsored by nation-states to achieve certain political goals. For example, in 2009-10, a computer malware known as the Stuxnet worm believed to have been created by the United States and Israel was used to slow down the progress of Iran's nuclear program. The Stuxnet worm reportedly affected computers in other countries such as India, Indonesia and Russia. It is also considered the first known worm produced to target real-world infrastructure like power stations, water plants and industrial units. Distributed Denial of Service (DDoS) attacks are increasingly becoming sophisticated and are being deployed as political weapons. Nation-states increasingly use cyberattacks and breaches to further their agenda and this has led to the explosion of new threats that require workable defenses for networks. For example, India, like any other nation may be targeted for cyber attack by another nation for its political interest.

Evolution of Cyber Laws in India:

The Indian parliament considered it necessary to give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL). As a consequence of which the Information Technology Act 2000 was passed and enforced on 17th May 2000. The preamble of this Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934**.** The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000 so that they may regulate and control the affairs of the cyber world in an effective manner.

The Information Technology Act deals with the various cyber crimes in chapters IX & XI. The important sections are Ss. 43, 65, 66, 67. Section 43 in particular deals with the unauthorised access, unauthorised downloading, virus attacks or any contaminant, causes damage, disruption, denial of access, interference with the service availed by a person. This section provide for a fine up to Rs. 1 Crore by way of remedy. Section 65 deals with '*tampering with computer source documents*' and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with '*hacking with computer system'* and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Further section 67 deals with publication of obscene material and provides for imprisonment up to a term of 10 years and also with fine up to Rs. 2 lakhs.

ANALYSIS OF THE IT ACT 2000 PROVISONS:

The Information Technology Act 2000 though was enacted at the right time which was the need of the hour then as there no legislation on the subject dealing with cyber crimes. But the Act as it is in its developing stage has been facing with a few loopholes which are:

1. That it was a hurriedly enacted legislation where no sufficient time was given for the public to have any effective debate on it.
2. It was basically enacted to facilitate the smooth functioning of e-commerce and never meant for cybercrimes, though incidentally, some of its provisions do mention about them.
3. The Act has not dealt with offences such as Cyber stalking cyber harassment, cyber nuisance, and cyber defamation which on the rise recently. However, the I.T. Act 2000 read with the Indian Penal Code 1860 is capable of dealing with these kinds offences.
4. As the present IT Act 2000 is insufficient to deal with Cyber Crime, a comprehensive law needs to be enacted which can take care of these crimes exclusively and we may not have to rely on other laws such as Indian Penal Code 1860.
5. Various definitions in the IT Act in relation to cyber crimes are clear and many times they are misleading. This may lead to misapplication of the definition. The Act needs to be suitably amended so as to include some of the important terms of cyber crimes. The Act also does not effectively deals with cyber pornography (*the Bal Bharati case*).
6. The most important reason for which the IT Act 2000 is not becoming successful is due to its lack of awareness. Many people do not even know that there is an Act called as IT Act. Due to this many cases go unreported.
7. Due to the universal nature of cyber crime, it does not recognize any geographical boundary. Though S.75 of the IT Act 2000 provides for extra-territorial operations of the Act, but an effective backing of proper provisions is missing.
8. The establishment of full fledged Cyber Crime Cells in all the major cities of the States is the need of the hour to fight the menace of cyber crime. In this direction he establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) by the Indian Government is certainly a welcome step.

Recommendations made to Government of India for amendments to the Information Technology Act, 2000.

Following is the summary of the recommendation made to the Government of India by the Asian School of Cyber Laws to deal with the menace of cyber crime more effectively and efficiently:

1. The Preamble to the Act needs to be amended to include addressing of cyber crimes as being one of the objectives of the Act.
2. Specific provisions relating to privacy and data protection be incorporated into a separate chapter.
3. The term credit card be defined appropriately in Sec. 43 and a specific provision providing for compensation to an aggrieved party for credit card frauds/thefts be incorporated under the said section.
4. Sction 509 of the Indian Penal Code, 1860 be amended suitably to accommodate Act r stalking and a provision should be inserted in section 43 of the IT Actto provide for compensation to a victim of cyber stalking.
5. An appropriate amendments may be made in the Gambling Prevention Act to address online gambling.
6. Section 65 be reworded to remove the ambiguity existing in the section as far as tampering with the computer source code is concerned.
7. Section 66 of the Act be suitably amended to penalize the creator of a harmful or malicious computer program (like virus etc.) and to make it applicable to data that is in transit.
8. Instead of specifically requiring the appropriate government to declare a computer system as being protected by notification, it would be appropriate to specify the category of "protected computer systems" in the Act itself.
9. Section 75 of the Act be amended to confer extraterritorial jurisdiction for offences committed and penalized under other statutes.
10. Sections 78 and 80 of the Act be amended to allow for investigation of offences registered under the Act by a police officer irrespective of his rank. This will lessen the burden on the shoulders of a high-ranked police officer for investigating each and every crime under the Act and at the same time allow for adequately addressing the grievances of an affected party at a much faster pace.

11. An additional provisions be included in the Act under chapter XII to clearly address the rights and liabilities of Network Service Providers so as to give impetus for investment in these areas.

Impact of Cyber Crime on the Criminal Justice system:
Cyber crime has made a significant impact on the criminal justice system prevalent throughout the world. The effects are seen even more as nations are constantly trying to provide faster and well-organized services to its citizens with the help of cyber space via internet. Almost all crimes in the modern time entail the use of computers and other electronic media at some stage of the act being committed by the offenders. Realizing the effectiveness of computers and the Internet to succeed in committing conventional crimes, the criminals are using them as tools for committing such criminal offences. There a Cyber Crime Investigation Cell is now the need of the hour for any law enforcement agency to tackle not only cyber crimes but also investigate other traditional or conventional crimes as there is an increasing use of encryption, high-frequency encrypted voice or data links, steganography etc. by terrorists and members of organized crime cartels. Some of the instances are coming to light where computers and other electronic tools have been used as tools to facilitate the commission of conventional crimes. Some of the conventional crimes where cyber space and other electronic media have been used are: Organised Crime, Terrorism, Cyber Crime

International Character of Cyber crime:
Cyber-crime is emerging as a major international criminological issue. Networked computers provide the media for new types (or variations on old types) of criminal activity to emerge. The widespread growth of cyber crime has affected nations from all across the globe. Incidents of cyber crime have caused extensive loss to a nation's economy. Loss of business profits and disruption of government and other services severely hampers the growth of any economy.

Cyber Crime and the Judiciary:
1. The **SONY.SAMBANDH.COM CASE** is One of the fist convicted cyber crime case in India is the case where a company called the Sony India Private Ltd, lodged a complaint for online cheating against one Mr. Arif Azim in 2002 at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The CBI recovered the colour television and the cordless head phone. The court of Shri Gulshan Kumar Metropolitan Magistrate, New Delhi, convicted him under Section 418, 419 and 420 of the Indian Penal Code, but since he was a young boy of 24 years and a first-time convict, he was released the accused on probation for one year.

2. Another first case in which a juvenile accused was involved is the case filed in April 2001 when a person from New Delhi complained to the crime branch regarding the website Amazing.com. He claimed that it carried vulgar remarks about his daughter and a few of her classmates. During the inquiry, print-outs of the site were taken and proceedings initiated. After investigation a student of Class 11 and classmate of the girl was arrested. The metropolitan magistrate Santosh Snehi Mann said: 'The mental condition under which the juvenile came into conflict with the law shall be taken into consideration during the final order.' Mann, however, dropped the sections of Indecent Representation of Women (Prohibition) Act and the accused was ordered to face trial under the Information Technology Act.

3. In the State of Tamil Nadu Vs Suhas Katti which is one of the first case in which there was a convicted under Information Technology Act 2000 of India, there was a posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet. On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC. The court came to the conclusion that the crime was conclusively proved. The accused was convicted and was sentenced to undergo RI for 4 years and 1 Simple Imprisonment under both IT Act and IPC and to pay a total fine of Rs.5000/-

4. In this case a Pentacostal Church priest and his son were sentenced to RI in 2006 for finding them guilty of morphing, web-hosting and e-mailing nude pictures of Pastor Abraham and his family with fake e-mail IDs with captions. Disposing of the appeal filed by the priest and his son, the Additional District Judge T.U. Mathewkutty said it was time the government took effective measures to check the growing trend of cyber crimes in the State. The court upheld the magistrate's order sentencing the two to three-year rigorous imprisonment and imposing a fine of Rs. 25,000 under Section 67 of the information technology (IT) Act; awarding six months rigorous imprisonment under Section 120(B) of the Indian Penal Code; and ordering one year rigorous imprisonment and imposing a fine of Rs. 10,000 under Section 469 of the code.

5. In yet another case one Dr. L Prakash a well-known orthopaedist in Chennai stood convicted of manipulating his patients in various ways, forcing them to commit sex acts on camera and posting the pictures and videos on the Internet. He landed in the police net in December 2001 when a young man who had acted in one of his porn films lodged a complaint with the police. Apparently the doctor had promised the young man that the movie would be circulated only in select circles abroad and had the shock of his life when he saw himself in a porn video posted on the web. Subsequent police investigations opened up a Pandora's box. Prakash and his younger brother, settled in the US, had piled up close to one lakh shots and video footages, some real and many morphed. They reportedly minted huge money in the porn business. The Fast track court judge R Radha, who convicted all the four in Feb 2008, also imposed a fine of Rs 1.27 lakh on Prakash, the main accused in the case, and Rs 2,500 each on his three associates - Saravanan, Vijayan and Asir Gunasingh. The Judge while awarding life term to Prakash observed that considering the gravity of the offences committed by the main accused, maximum

punishment under the Immoral Trafficking Act (life imprisonment) should be given to him and no leniency should be shown. The Judge sentenced Prakash under the Immoral Trafficking Act, IPC, Arms Act and Indecent Representation of Women (Prevention) Act among others.

6. In Pune Citibank MphasiS Call Center Fraudcase a sum of US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced.

7. In Bazee.com case the CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai and the Delhi Police got into action. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider.

8. The Bank NSP Case: In this case a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email IDs such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to Court. The bank was held liable for the emails sent using the bank's system.

9. In SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra case which is India's first case of cyber defamation, the defendant being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff. The Honb'le Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further,

10. In PARLIAMENT ATTACK CASE, the Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13, 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

11. In the Andhra Pradesh Tax Case, the Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days. The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

12. In the landmark judgment of the National Association of Software and Service Companies (**Nasscom) vs. Ajay Sood & Others, decided in** March, 2005, the Delhi High Court stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. This case has brought the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation;

A careful analysis of the above mentioned few cases show that our criminal justice system has a long way to go to improve itself inorder to fight againsy Cyber Crimes. In other words, even though we have markedly improved our capabilities to fight cyber intrusions so far, but the problem of cyber crime is growing even faster and we are falling further behind**.** Anyway one thing is for sure that there is always room for improvement.

Cyber Crime Prevention: Challenges ahead:

"*To fight and win all your battles is not the acme of excellence. Supreme excellence lies in subduing your enemy without fighting*" – *Sun Tzu.*

Sometimes we often wonder how wired connected we are with each other. Almost everything in our life is connected to some kind of technology and its gadgets. But imagine what a hacker can do to our life. He can snap down all our connections and turn us into Stone Age within minutes for hours together. This is in what is called as the cyber war in the modern terminology. Therefore, to fight this war our criminal justice system must be alert.

Cyber crime is the new challenge for the Indian society, industry and the law enforcement and the entire criminal justice system as a whole. The anonymous nature of the Internet makes it an attractive medium to commit crimes and frauds. Cyber crime is not confined to any national

boundary. Therefore, it becomes very difficult to control the extent of its criminal activity. Though cyber crimes are increasing day by day and has become a matter of concern, yet there is lack of awareness among the people in general. Many individuals do not take initiative to come and report these crimes either due to its lack of awareness or in their opinion; such crimes would not be given much significance. Moreover, even some organizations also hesitate in reporting such crimes as they are afraid of losing reputation in the market.

The present position shows that cyber crimes are likely to grow in extent and complexity as more and more people are accessing internet services for their various purposes. It is high time that industries, law enforcement agencies and supporting groups should come forward to empower and protect individuals and organisations from falling prey to these cyber crimes and other online crimes.

The Police personeel, the prosecutors and the lower judiciary need to be educated to fight cyber crimes. This can be effectively achieved by organizing periodic conferences, seminars and workshops, training programmes, etc. In fact the CBI, the Bureau of Police Research and Development (BPR&D) and the National Police Academy (NPA), Hyderabad have already made significant contributions by preparing a training module to be administered to State police personnel and conducted several training programmes. There is no information that any systematic effort has been made till now to impart training to prosecutors and judges, although there is evidence of their keenness to become knowledgeable.

An International co-operation in fighting the menace of cyber crime is the need of the hour today as the cyber crime knows no boundaries. For example, a hacker in New York can break into a system in Mumbai without the aid of any extraordinary talent or equipment. What he needs is a personal computer and a network connection. There is a need create a an awareness among the international community that a hacker should not be allowed to get away only because of legal inadequacies. Section 75 of the IT Act clearly lays down that its provisions shall also apply to "any offence or contravention committed outside India by any person, irrespective of his nationality", provided that such act involves a computer, a computer system or computer network located in India.

But the biggest problem in securing international co-operation is that some nations are trying to protect their own citizens once a blame comes on them. The procedure also involves a request by the court of one country to its counterpart in another. Collection of information in cyber matters requires searches and confiscation of delicate material that needs speedy and expert handling. Assistance in such areas is slow and half-hearted despite the best of relations between countries.

The Commission on Crime Prevention and Criminal Justice (CCPCJ) of the United Nations, with its headquarters in Vienna, has been exercised over how to prevent and control high technology and computer-related crime. The Commission is convinced that one way of doing this is to forge closer links between nations so that the cyber criminal is relentlessly pursued across frontiers. Both the Eighth U.N. Crime Congress and the Tenth one devoted considerable time to this.

The U.N. Convention on Transnational Organised Crime adopted by the General Assembly on November 15, 2000 may not directly apply to routine computer crime. However, it will definitely be attracted where organised gangs use telecommunication and computer networks for their operations. Following this Convention, the CCPCJ held a workshop on "The Challenge of Borderless Cyber Crime" in December 2000 at Palermo, Italy. The workshop, attended by representatives of a large number of countries, gave a fillip to the movement that aims to strengthen the law and procedure for international cooperation in the field.

The Lyon Group of high-level experts set up by the G-8 nations has also been active. At this group's instance, a network of contacts available round-the-clock has been established. The Interpol has now the operational responsibility for this network and the CBI has been identified as a contact point for the Indian subcontinent and its neighbourhood.

In sum, an ambience has no doubt been created for promoting international cooperation to combat cyber crime. How far this will translate itself into active assistance in the field is an open question. Going by the track record of many countries in tackling more serious transnational criminals - such as Dawood

Ibrahim and his class - we may not expect miracles. A change of mindset is called for. It will definitely come when nations are overtaken by a rash of major cyber misdeeds which impinge on national security and threaten critical infrastructure. Meanwhile, we in India will have to disseminate zealously knowledge of how to protect our computer systems and encourage freer reporting by victims to police agencies. As it is, there is gross underreporting, alongside a tendency towards vigilantism. Both tendencies need to be curbed.

Network Service Provider's Liability:

The Information Technology Act, 2000 provides that the Network Service Providers (ISPs)not to be liable for any third party information made available by him, if, he proves that the offence was committed without his knowledge, or that he had exercised all due diligence to prevent the commissioning of such offence. The reason behind this is that the ISPs have no control over the contents of websites that are accessed daily.

Then the question is who is liable for the unlawful acts on the Internet. Is it the sender of the information, the service provider, the user or all of them together? In the Church of Scientology case in the Netherlands, the court decided that the information providers do nothing more than offer an opportunity to publish and that they are unable to exercise any control over, or even be aware of, what people say or are able to say on the internet. Another problem is that if the service providers tries to constantly monitor the all the sites on his server, it may amount to undesirable form of censorship by him.

But it the service provider is the only one person apart from the information provider himself, who can prevent the crime being committed by way of closing the site. At the same time every possible thing should be done to trace the source of the information. And hence it is the source and not the service provider primarily is liable for the content. But sometime the service provider may be held responsible by

compelling him to reveal the identity of the owner of anonymous home page during investigation.

Cyber Terrorism and the ISP liability: The Anti-Terrorism, Crime and Security Act, 2001 was passed in UK as an emergency legislative measure in the wake of the September 11 terrorist attacks. The Act provides for a code of practice on the retention by the ISPs, etc, of communications data obtained held by them such as websites visited by the customers and when and to whom emails are sent would also be retained. The data will be made available on the request to law enforcement agencies for the purpose of safeguarding, or preventing or detecting crime that related to, national security.

Measures to prevent Cyber Crimes: An attempt has been made by the author to give some suggestion as to how cyber crime can be avoided.

1. In the case of organizations:

A. The first step must be to begin the process of fully understanding the organisation's exposure to the threat of data/information. For instance, at the time of recruitment of staff, the organization must make sure that they must have an adequate background.
B. There must by reasonable restrictions imposed on the employees' access to data based on their role and there must be adequate control on their activities.
C. Adequate training must be provided to the employees in cope up with cyber crime threats and to report immediately their incidents.
D. There is a need to make Acts like Data Protection Act (DPA), HIPPA, etc., mandatory for Indian companies.
E. There is a need for an effective process such as information sharing and cooperation with foreign countries as cyber crimes are not confined to geographic borders.
F. The Companies must register themselves with the CERT to stay updated with latest vulnerability and treats.
G. They need to conduct user awareness programs periodically.
H. They must update their security polices and procedures regularly.
I. They must perform security audit and implement suitable recommendations.
J. Companies must adopt global security practices so as to encourage more and more people to prefer online transactions.

2. In the case of Law Enforcement Agencies:

A. At the outset there is an urgent need to introduce Graduation an one of the minimum qualification for the police personnel.
B. Basic computer training is a must for the newly recruited police personnel.
C. The Law enforcement officers must be provided with adequate training in various broad range of issues relating to
   1. cyber crime,
   2. forensic work,
   3. online sharing procedures and communication protocols. Such training needs to be conducted more frequently for the law enforcement officials so that enforcement units are capable of investigating cyber crime.

D. Some of the basic skills required by the law enforcers are:
   1. Common forensic computing techniques;
   2. automation of digital evidence analysis;
   3. procedures for data recovery and analysis;
   4. legal considerations;
   5. principles of forensic computing;
   6. disk and file system forensics;
   7. operating systems forensics; and
   8. Internet and organisational networks.

E. Finally, for the complete realisation of the provisions of the cyber laws, a cooperative police force is required to encourage victims to report cyber crimes.

3. **In the case of individuals:**

A. There must be proper user awareness programmes conducted to educate the people about the seriousness of cyber crime and its prevention.

B. A counseling session for college students has to be launched to educate them on the gravity and consequences emanating from cyber crimes.

C. Individuals must avoid giving out any personal information about themselves to any one specially the strangers.

D. Children should never be allowed to arrange their face-to-face meetings or send their photographs online without informing their parents.

E. The latest and updated anti-virus software, operating systems, Web browsers and email programs must be used to fight against virus attacks.

F. One must always thoroughly check the site he is doing business with.

G. On must send credit card information only to secured sites.

H. While chatting on the net one should avoid sending photographs to strangers along with personal data as it can be misused.

I. * Backup volumes of the data should always be kept to prevent loss from virus contamination. * Children should be prevented from accessing obscene sites by the parents to protect them from spoiling their mind and career. * A credit card number shall never be sent to an unsecured site to prevent fraud or cheating. Effort shall be made to make a security code and program to guard the computer system from misuse.

J. We must use a security program that gives us a control over the cookies that send information back to Web sites. Letting all cookies in without monitoring them could be risky.

K. If you own a Web site, watch traffic and put host-based intrusion detection devices on your servers. Monitor activity and look for any irregularities.

L. Put in a firewall and develop your content off line.

M. * A check should be kept on the functioning of cyber cafes and any mishappening shall be reported to the concerned authorities. *Efforts should be made to discourage misuse of computers and access to unauthorized data.

4. Cyber Café's: Though the cyber café' owners cannot be held liable for anything done by any person accessing the internet without their knowledge, but it is their duty to keep due records about the customers. They can do it by maintaining a register wherein the customers can enter their names, addresses, phone numbers, etc. The can also be allowed to enter the café' only by checking their ID cards if any, etc. This will enable them to keep track of their suctomers.

Cyber Crime and Global Co-operation: Issues of jurisdiction have quickly come to the fore in the era of the digital world and the Internet. A single Internet transaction may involve the laws of at least three countries: i) laws of the user country, ii) country where the server is hosted; and iii) merchant/business country with whom the transaction takes place.

So it is vital for international law enforcement agencies to cooperate to implement measures to investigate, capture and prosecute cyber criminals.

Parliament passed the IT Bill in May 2000, notified it as the IT Act 2000 in order to bring e-commerce within the purview of the law and accord stringent punishments to cyber criminals.

Conclusions:

Change is the essence of life. What seems impeccable and indestructible today might not remain the same tomorrow. Internet, being a global phenomenon is bound to attract many crimes. India has taken a key step in curbing Cyber Crimes by the enactment of the Information Technology Act and by giving exclusive powers to the police and other authorities to tackle such crimes.

Similar efforts have been made by various countries to fight this menace by enacting national legislations but in the long run, they may not prove to be as beneficial as desired. An effort is still wanted to formulate an international law on the use of Internet to curb this imminent danger of Cyber Crimes and to achieve a crime free Cyber Space. Prevention they say is the best cure. Cyber laws aim to prevent cyber crimes through the use of penal provisions. A great deal however needs to be done before Cyber laws can stand a fair chance to influence the modern.

References

[1] Vakul Sharma, *Handbook of Cyber Laws*, First ed., 2002, Macmillan India Ltd, New Delhi, page 126.

[2] Byrne, J. and Burton, P. (2017). "Children as Internet users: how can evidence better inform policy debate?", *Journal of Cyber Policy*, 2 (1): 39 - 52.

[3] Nitant P. Trilokekar, *A Practical Guide to Information Technology Act, 2000*, Snow White Publications Pvt. Ltd., 2000, Mumbai, p.212.

[4] Wall, D.S. (2001). "Cybercrimes and the Internet". In D.S. Wall (Ed.). *Crime and the Internet*, pp. 1-17. New York: Routledge.

[5] Safa, N.S., Maple,C., Watson, T. and Sloms, R. V. (2018). "Motivation and opportunity based model to reduce information security insider threats in organizations". *Journal of Information Security and Applications*.

[6] Brenner, S.W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. California: Praeger.

[7] Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer: Law and Business.

[8] Sviridoff, M. and Thomposn, J.W. (1983). "Links between employment and crime: A qualitative study of Rikers Island Releasees". *Crime and Delinquency*, pp.195-212.

[9] Ndubueze, P.N. (2017a). "Generation Y and online victimization in Nigeria: How vulnerable are younger internet users". In K. Jaishankar (Ed.). *Interpersonal Criminology: Revisiting Interpersonal Crimes and Victimization*. pp. 203 - 214. Boca Raton: CRC Press, Taylor & Francis Group.

[10] Field, S. (1990). *Trends in crime and their interpretation: A study of recorded crime in post- war England and Wales*. Home Office Research Study, 119. London: HMSO.

[11] Maslow, A. (1945). "A theory of human motivation". *Psychological Review*, 50: pp.370- 396.

[12] Merton, R.K. (1938). "Social structure and anomie". *American Sociological Review*, 3:pp.672-682.

[13] Mansfield-Devine, S. (2017). "Ransomeware: Taking businesses hostage". *Network Security*, (10): pp.8-17

[14] Presdee, M. (2000). *Cultural Criminology and the Carnival of Crime*. London: Routledg

[15] Rodney D, Rider (2007), *Guide to Cyber Laws*, Third Ed., Wadhwa and Company, Agra, Nagpur & New Delhi, p.1173.

[16] Kigerl, A. (2012). "Routine Activity Theory and the determinants of high cybercrime countries". *Social Science Computer Review*, 30 (4): pp.470 - 486.

[17] Everett, C. (2009). "The lucrative world of cyber-espionage". *Computer Fraud and Security*, 2009 (7): pp.5-7.

[18] Chaudhry, P. E. (2017). "The looming shadow of illicit trade on the internet". *Business Horizon*, 60 (1), pp.77-89.

[19] Clough, J. (2015). *Principles of Cybercrime*. Cambridge: Cambridge University Press.

[20] Lavorgna, A. (2015). "Organized Crime Go Online: Realities and Challenges". *Journal of Money Laundering Control*, 18 (2):pp.153- 168.

[21] Leukfeldt, R. (2015). "Organized Crime and Social Opportunity Stuctures: A Proposal for Future Research Directions". *The European Review of organized Crime*, 2 (2): pp.91-102.

[22] O'Conncell, M.E. (2012). "Cyber security without cyber war". *Journal of Conflict & Security Law*, 17 (2): pp.187 – 209.

[23] Mansfield-Devine, S. (2015). "The growth and evolution of DDoS". *Network Security*, (10): pp.13-20.

[24] Lundbohm, E. (2017). "Understanding nation-state attacks. Network Security", 2017 (10): pp.5-8.

Websites

[1] http://www.thehindubusinessline.com/mentor/2007/05/21/stories/2007052100681300.html.

[2] Available at http://www.hinduonnet.com/fline/fl1816/18161040.htm

[3] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

[4] www.alertindian.com/node/18

[5] http://www.indiacyberlab.in/know_more/copawards2005-message.htm

Articles

[1] The New Indian Express, 21/06/2008, p.8.